Notice of Allowability	Application No.	Applicant(s)	
	10/076,199	FILIPI-MARTIN ET AL.	
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *21 May 2007*.

2. ☒ The allowed claim(s) is/are *1-3 and 7*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. Claims 4-6 and 8-19 have been cancelled.

2. Claims 1-3 and 7 have been amended.

3. Claims 1-3 and 7 are pending.

Response to Arguments

4. Applicant's arguments filed 21 May 2007 have been fully considered and they are persuasive.

Allowable Subject Matter

5. **Claims 1-3 and 7** are allowed.

6. The following is an examiner's statement of reasons for allowance: The present invention is directed toward a method and system for an automated electronic encryption system and for managing key pairs, encrypting electronic transmissions over a network between senders and recipients of secure domains and senders and recipients of non-secure domains, and intercepting an electronic message from an e-mail client without e-mail client processing. Claim 1 identifies the uniquely distinct features "**a set of computer readable encryption instructions embodied within a computer readable medium to receive the electronic message from the e-mail client prior to encryption of the e-mail and attempting to decrypt the sender's private key according to the recipient's ID and password, encrypting the electronic message for subsequent retrieval so that the electronic message is automatically encrypted and delivered to the recipient without the need for the email client to retrieve the recipient's public key or encrypt the message**".

The closest prior art, O'Brien et al. (US Patent No. 6,990,578) discloses a method and apparatus for encrypting electronic messages composed using abbreviated address books, when electronic mail is to be sent by an off-line user to a recipient who holds a digital certificate, the sender's mail program allows the sender to compose the mail, but the mail is placed in plain text in the sender's local outbox and flagged for subsequent encryption. When the sender later connects to a mail server to send the outgoing mail, the sender's mail software, in response to the flagged mail will request the recipient's certificate from the server and use the received certificate to encrypt the mail message before it leaves the sender's workstation. In accordance with one embodiment of the invention, after using a digital certificate to encrypt a mail message, the certificate is discarded. In accordance with another embodiment, if the certificate is not available or located by the mail server, a message is sent to the sender informing him that the certificate cannot be located and the mail cannot be sent in encrypted form. At that point, the sender has an option to resend the mail in unencrypted form.

However, either singularly or in combination, O'Brien et al. fail to anticipate or render the claimed limitation wherein intercepting the e-mail as it is sent from the e-mail client to a server to perform the encryption, the e-mail client not required to retrieve a certificate or encrypt the message and performing any processing of encryption at the e-mail client.

The closest prior art, Meffert et al. (Pub No. 2002/0059144) discloses a system for and method of automatically implementing PKI-based encryption between a sender and a recipient. The system includes a sender local agent associated with a sender

electronic device and a recipient local agent associated with a recipient electronic device wherein both the sender and recipient electronic devices are capable of connecting to a control server via the Internet. The sender local agent is operable to (i) receive content generated on the sender electronic device, (ii) generate a package of encrypted content using PKI-based encryption by obtaining at least one public key from the control server, and (iii) send the package to the control server. The control server is operable to receive the package from the sender local agent and transmit the package to the recipient local agent. The recipient local agent is operable to (i) receive the package from the control server, (ii) launch a recipient local agent-controlled window or process, (iii) decrypt the encrypted content in the package, and (iv) use or display decrypted content within the recipient local agent-controlled window or process. Packages preferably include content such as text, data and graphic images. Packages also preferably include embedded content dissemination rules, selected by the package sender, restricting the dissemination of the content by the recipient.

However, either singularly or in combination, Meffert et al. fail to anticipate or render the claimed limitation wherein intercepting the e-mail as it is sent from the e-mail client to a server to perform the encryption, the e-mail client not required to retrieve a certificate or encrypt the message and performing any processing of encryption at the e-mail client.

The closest prior art, Meffert et al. (Pub No. 2003/00397261) discloses a system and method for secured content delivery between a sender and a recipient in an electronic network using PKI-based encryption. The system includes a sender local

agent associated with a sender electronic device and a recipient two-factor authentication associated with a recipient wireless device wherein both the devices are capable of connecting to a control server via the Internet. The sender local agent is operable to (i) receive content generated on the sender electronic device, (ii) generate a package of encrypted content using PKI-based encryption by obtaining at least one public key from the control server, and (iii) send the package to the control server. The control server is operable to receive the package from the sender local agent and transmit the package to the recipient local agent. The recipient two-factor authentication is operable to (i) receive the packet from the control server, (ii) prompt the recipient to enter a user PIN, (iii) responsive to receiving the user PIN, generate a one-time passcode that is valid within a predetermined interval, and (iv) accessing to the network within the predetermined interval using both the user PIN and the one-time passcode.

However, either singularly or in combination, Meffert et al. fail to anticipate or render the claimed limitation wherein intercepting the e-mail as it is sent from the e-mail client to a server to perform the encryption, the e-mail client not required to retrieve a certificate or encrypt the message and performing any processing of encryption at the e-mail client.

The closest prior art, Srinivasan (Pub No. 2003/0126085) discloses a system and method for dynamic authentication of a digital signature included in an electronic message are provided. The sender sends a certificate reference together with a digitally signed electronic message. The certificate reference uniquely maps to a certificate stored in a public key infrastructure (PKI). Upon receipt of the message, including the

certificate reference, the recipient requests the certificate from the PKI by sending the certificate reference to the PKI. The PKI responds by mapping the certificate reference to the corresponding certificate and providing the certificate, which may then be used to authenticate the digital signature.

However, either singularly or in combination, Srinivasan fail to anticipate or render the claimed limitation wherein intercepting the e-mail as it is sent from the e-mail client to a server to perform the encryption, the e-mail client not required to retrieve a certificate or encrypt the message and performing any processing of encryption at the e-mail client.

7. Therefore, **claim 1** and the respective **dependent claims 2-3 and 7** are in condition for allowance.

Conclusion

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

cdf
July 31, 2007

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137